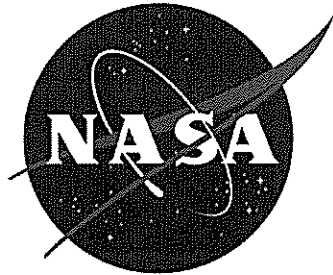


# **NASA Information Technology Requirement**



**NITR 2810-17**

Effective Date: November 12, 2008

Expiration Date: May 16, 2011

---

## **System Maintenance Policy and Procedures**

---

Responsible Office: Office of the Chief Information Officer

## **Table of Contents**

### **PREFACE**

- P.1 PURPOSE
- P.2 APPLICABILITY
- P.3 AUTHORITY
- P.4 APPLICABLE DOCUMENTS
- P.5 MEASUREMENT AND VERIFICATION
- P.6 CANCELLATION

### **1.0 REQUIREMENT**

- 1.1 System Maintenance Policy
- 1.2 Procedures

### **APPENDIX A. Definitions**

### **APPENDIX B. Acronyms**

### **Distribution:**

### **NODIS**

## **PREFACE**

### **P.1 PURPOSE**

a. To provide the NASA information system maintenance policies and procedures to meet the current National Institute of Standards and Technology (NIST) requirements.

### **P.2 APPLICABILITY**

a. This NITR applies to unclassified information systems at NASA Headquarters and Centers, including Component Facilities and Technical and Service Support Centers. To the extent specified in their respective contracts or agreements, it applies to the NASA Jet Propulsion Laboratory, other contractors, grant recipients, or parties to agreements for information systems that they use or operate on behalf of the Agency or that support the operations and assets of the Agency.

### **P.3 AUTHORITY**

a. Reference Paragraph P.3, NPR 2810.1A.

### **P.4 APPLICABLE DOCUMENTS**

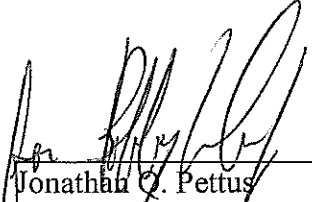
- a. NPR 2810.1A, Security of Information Technology
- b. Federal Information Processing Standard (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems.
- c. NIST SP 800-100, Information Security Handbook: A Guide to Managers.
- d. NIST SP 800-53 Revision 2, Recommended Security Controls for Federal Information Systems.
- e. NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems.
- f. NIST SP 800-37, Guide for Security Certification and Accreditation of Federal Information Systems.

### **P.5 MEASUREMENT AND VERIFICATION**

- a. Annual certification of the Agency Common Security Control MA-1, System Maintenance Policies and Procedures.
- b. Annual assessment of the Agency MA-1 common security control by the Information System Owner (ISO) as part of the system Continuous Monitoring requirements

### **P.6 CANCELLATION**

- a. The next version of NPR 2810.1 cancels this NITR.

  
Jonathan Q. Pettus  
NASA Chief Information Officer

11/12/08  
Date

## **1.0 REQUIREMENT**

### **1.1 System Maintenance Policy**

1.1.1 A formal maintenance policy shall be developed, reviewed annually and updated as needed.

1.1.2 The maintenance policy shall be consistent with applicable laws, Executive Orders, directives, regulations and guidance.

1.1.3 The maintenance policy shall include:

- a. Information about the purpose and scope as well as the roles and responsibilities of individuals responsible for actions.
- b. Details of the implementation.
- c. A configuration management process that includes Configuration Control Board (CCB) change control for tracking, managing, and approving any maintenance activity that results in hardware or software changes to the system.
- d. A list of the specific systems to which the policy applies.
- e. Procedures for scheduling maintenance that comply with the contingency planning policy.
- f. A limit on maintenance personnel to the smallest possible number.
- g. Allowing only authorized maintenance personnel to perform maintenance on NASA information systems and have the appropriate access authorizations.
- h. That maintenance tools brought in specifically for diagnostic/repair actions of Moderate or High category information system for be approved, controlled, maintained, and monitored.
- i. Scheduling, controlling, tracking, and documenting all preventative and regular maintenance.

1.1.4 The maintenance policy shall include the following requirements:

- a. Maintenance personnel must obtain written approval from the ISO for each maintenance activity or repair before they perform it.
- b. A report of any significant system changes will be sent to the Center Information Technology Security Manager (ITSM).

### **1.2 Procedures**

1.2.1 The Center Chief Information Officer (CIO) shall:

- a. Establish a Center maintenance policy that implements the above Agency policy.
- b. Maintain oversight of the maintenance policy implementation by the Center ISOs.

1.2.2 The Information System Owner (ISO) shall implement the organization's system maintenance policy and use them to assess the system's Maintenance security controls.

1.2.3 The Senior Agency Information Security Officer (SAISO) shall:

- a. Annually review, and update as required, the System Maintenance Policy and Procedures as part of the annual review of the MA-1 control as an Agency common control providing management oversight to assure policy currency and compliance.
- b. Annually certify the MA-1 Agency common control to assure it satisfies the purpose, scope, and compliance requirements for system maintenance.

## APPENDIX A. Definitions

Term	Definition
Certification	A formal process for testing components or systems against a specified set of security requirements. Certification is normally performed by an independent reviewer, rather than one involved in building the system. Certification is more often cost-effective for complex or high-risk systems.
Common Control	A security control that is inherited by an information system
Configuration Control	Process for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during, and after system implementation. [CNSS Inst. 4009]
Continuous Monitoring	Refers to a phase of the Certification and Accreditation Process of Information Systems. It consists of three tasks: (i) configuration management and control; (ii) security control monitoring; and (iii) status reporting and documentation. The purpose of this phase is to provide oversight and monitoring of the security controls in the information system on an ongoing basis and to inform the authorizing official when changes occur that may impact on the security of the system. The activities in this phase are performed continuously throughout the life cycle of the information system.
Hybrid Security Control	A security control that is part common control and part system-specific control
Information System (Also referred to as IT System)	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information in accordance with defined procedures, whether automated or manual. [OMB Circular A-130, Appendix III]
Information System Owner	An agency official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. Responsible for the development and maintenance of the system security plan and ensures the system is deployed and operated according to the security requirements.

Term	Definition
Security Category	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operation, organizational assets, individuals, other organizations, and the Nation. [FIPS 199 as amended by NIST SP 800-53]
Senior Agency Information Security Officer	Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers. [44 U.S.C., Sec. 3544] Synonymous with Chief Information Security Officer (CISO)
Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system which, taken together, satisfy the specified security requirements and adequately protect the confidentiality, integrity, and availability of the system and its information.
Site Control or Site Common Control	An inherited security control from a common site that usually applies to multiple information systems. Example is when more than one system is operating from a common data center (site) and information system owners are required to use that sites' security controls, e.g. site access control, site power, etc.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information in accordance with defined procedures, whether automated or manual. [OMB Circular A-130, Appendix III] (Also referred to as IT System)

## **APPENDIX B. Acronyms**

CCB	Configuration Control Board
CIO	Chief Information Officer
CM	Configuration Management
FIPS	Federal Information Processing Standards
ISO	Information System Owner
IT	Information Technology
ITSM	Information Technology Security Manager
NIST	National Institute of Standards and Technology
NITR	NASA Information Technology Requirement
NPR	NASA Procedural Requirements
OCIO	Office of the Chief Information Officer
SAISO	Senior Agency Information Security Officer
SP	Special Publication